INTERNET AUTHENTICATION WITH MULTIPLE INDEPENDENT CERTIFICATE AUTHORITIES

ABSTRACT OF THE DISCLOSURE

A system for authentication to support secure data transfer includes a protocol wherein a certificate payload, an ID payload, and a signature payload all respectively contain at least two certificates, IDs, and signatures, concatenated together. The certificates are generated by different certificate authorities (CA) that have no trust relationship with each other. One certificate can be granted to a person and another to a particular host computer intended to be used by the person, so that for secure data transfer to take place, both a certified user and a certified host computer must be involved.